Freie Universität Berlin

{tip4u://184} Version 5

Zentraleinrichtung für Datenverarbeitung (ZEDAT)
www.zedat.fu-berlin.de

CEO Fraud

Über gefälschte, angeblich von Vorgesetzen stammende Nachrichten versuchen Kriminelle gezielt, Geld zu erbeuten.

zedat

Zentraleinrichtung für Datenverarbeitung
Fabeckstraße 32 / 14195 Berlin
Hotline (030) 838 77777 / service@fu-berlin.de

Gefälschte Anfragen von Vorgesetzten (CEO Fraud)

Gefälschte Nachrichten von angeblichen Vorgesetzten, die sich mit der Bitte um Hilfe gezielt an Mitglieder des jeweiligen Bereichs wenden, sind eine beliebte Masche von Trickbetrügern, mit der diese versuchen, schnell große Summen zu erbeuten.

„CEO Fraud" gibt es sowohl in Deutsch als auch in Englisch. In keinem Fall sollte auf derartige Betrugsversuche eingegangen werden!

English language example at the end of this document. Please read and be warned!

Spielarten von Phishing Mails

Gefälschte E-Mail-Nachrichten sind ein Ärgernis und können ein hohes Sicherheitsrisiko darstellen. Neben den herkömmlichen, im Tip4U #183[1] beschrieben Phishing Mails, bei denen es um die Erbeutung von Zugangsdaten geht, gibt es vermehrt zielgerichtete Angriffe wie den sogenannten „CEO Fraud".

Die Abkürzung „CEO" steht im englischsprachigen Raum für „Chief Executive Officer", der Begriff „fraud" lässt sich mit „Betrug" oder „Schwindel" übersetzen. Es handelt sich bei diesem Angriff also um einen gezielten Betrug, bei dem sich Kriminelle als Vorgesetzte ausgeben und versuchen, sich auf Kosten ihrer Opfer zu bereichern.

Masche

Die Betrugsmasche ist relativ einfach: Es geht darum, eine Nachricht als vermeintlich Vorgesetzter zu versenden, darum zu bitten, dass „mal eben schnell" z.B. Geschenkgutscheine erworben und die Nummern derselben dann auch gleich per Mail weitergeleitet werden.

Selbst wenn das einfach zu durchschauen klingt, entsteht an vielen Einrichtungen – auch an Universitäten – dadurch erheblicher finanzieller Schaden. Im folgenden Abschnitt wird an zwei Beispielen veranschaulicht, wie sich Trickbetrüger nach und nach annähern. Es handelt sich dabei um sehr gezieltes sogenanntes „Social Engineering". Da es in vielen Arbeitsgruppen an der Freien Universität Berlin auch englischsprachige Angehörige gibt, folgt ein warnendes Beispiel in beiden Sprachen.

[1] https://zedat.fu-berlin.de/tip4u_183.pdf

Beispiel: CEO Fraud auf Deutsch

Die erste Nachricht ist ganz unverfänglich und lockt das Opfer ins Boot.

```
Von: Prof. E. Muster <leitung4711@gmail.example>
An: erwin_piependeckel@fu...
Betreff: DRINGEND

Hallo Erwin!  Bist du verfügbar ?

Prof. Dr. Erika Muster
Freie Universität Berlin
Institut für Angewandte Freiluftforschung, Zimmer JK 47/11
Beispielstraße 12, 14195 Berlin, Germany
```

Die Daten in der Signatur sind echt und stammen z.B. von einer offiziellen Seite der Universität; Professorin und angeschriebener Mitarbeiter gehören zur gleichen Arbeitsgruppe. Vielleicht werden auch noch weitere Mitglieder der AG auf der Webseite genannt, die dann parallel von den Kriminellen in separaten Mails mit angeschrieben werden.

Die Mail kommt zwar von einer Absenderadresse, die nicht zur Freien Universität Berlin gehört, der Rest der Mail ist aber darauf angelegt, dass den Opfern bei einem schnellen Querlesen keine Bedenken kommen. Der Text ist kurz und an sich nicht verdächtig, sodass sich die Nachricht den zentralen Filterkriterien der Mailserver entzieht.

Das Opfer hält die Mail für echt und antwortet so schnell wie möglich auf die Kurzanfrage der vermeintlichen Vorgesetzten. Ob es das auf Deutsch oder Englisch tut, ist nicht von Belang. Die Angreifer sind flexibel und gehen darauf ein.

```
Von: ”Piependeckel, Erwin” <erwin_piependeckel@fu...>
An:  Prof. E. Muster <leitung4711@gmail.example>
Betreff: AW: DRINGEND

Hallo Frau Prof. Muster,

ja, ich bin jetzt erreichbar, was kann ich für Sie tun?

Mit freundlichen Grüßen

Erwin Piependeckel
Wissenschaftlicher Mitarbeiter
Freie Universität Berlin
Institut für Angewandte Freiluftforschung
```

Das Opfer ist auf die Kommunikation eingegangen und damit am Haken. Die zweite E-Mail der falschen Professorin folgt prompt, ohne dass die Katze schon aus dem Sack gelassen wird.

```
Von: Prof. E. Muster <leitung4711@gmail.example>
An: erwin_piependeckel@fu...
Betreff: Re: AW: DRINGEND

Sie müssen eine Aufgabe für mich diskret erledigen. Ich bin jetzt in
einer Besprechung. Anrufe sind verboten, daher kann ich Sie nur per
E-Mail kontaktieren. Ich habe keine Ahnung, wann wir die Dinge hier
erledigen werden. Ich brauche jedoch wirklich Ihre Hilfe bei etwas, das
meine dringende Aufmerksamkeit erfordert.

[...]
```

Ob darauf wieder geantwortet wird oder nicht, ist egal. Es folgt eine weitere Nachricht, die den eigentlichen Betrugsversuch enthält.

```
Von: Prof. E. Muster <leitung4711@gmail.example>
An: erwin_piependeckel@fu...
Betreff: Re: AW: DRINGEND

Sie müssen mir helfen. Geschenkkarten aus jedem Geschäft zu bekommen.
Ich werde Sie erstatten, wenn ich im Büro bin. Ich muss es an einen
Kollegen senden und es ist sehr wichtig, weil ich noch bei der
Besprechung bin und es so schnell wie möglich erhalten muss.  Kannst du
das bitte für mich tun?

[...]
```

Wenn nun – ggf. nach weiterem Mailwechsel – das Opfer Gutscheine im Internet oder im Laden kauft und die Codes an den vermeintlichen Chef schickt, ist es sein Geld los.

Gegenmaßnahmen

An der Freie Universität Berlin gibt es eine gut funktionierende Spam- und Viren-Erkennung, wodurch der persönliche Posteingang von vielen bösartigen E-Mails freigehalten wird. Bei der dargestellten Art von Angriffen ist es aber technisch unmöglich, die betrügerischen Nachrichten vollständig herauszufiltern.

Erhöhte Aufmerksamkeit und ein gesundes Misstrauen sind in diesen Fällen der beste Schutz.

Weitere Informationen zum Security- und Abuse-Management der ZEDAT finden sich unter:

https://www.zedat.fu-berlin.de/AbuseManagement

Informationen zu Personen-Zertifikaten, mit deren Hilfe E-Mails signiert und damit bei Empfängern zweifelsfrei als echt identifiziert werden können, finden sich unter:

https://www.zedat.fu-berlin.de/Zertifikate

Example: CEO Fraud in English

The first message is a door opener. It gets the victim involved:

```
From: John Doe <director2021fu@somewhere.example.org>
To: p_parker@fu...
Subject: Are you available?

Dear Petra,

I am in a meeting at the moment, but need your help. Do you have a minute?

Best, John

Prof. Dr. John Doe
Department of Advanced Science
Freie Universität Berlin
Example Street 45
14195 Berlin
```

Both the professor's and the victim's name are real. They are probably copied directly from an official webpage. Maybe the working group even has more potential victims listed on that page, then they may all be treated in parallel.

The mail itself is not from a university sender-address, but the rest triggers no bells. The message body is short and inconspicuous.

Petra is flattered she can help of course. She fails to double-check the sender's e-mail (or perhaps thinks the freemailer is the professor's private address that he uses on his cell phone) and answers promptly. Whether she writes in German or English is not important, the attackers have text blocks for both.

```
From: Petra Parker <p_parker@fu...>
To: John Doe <director2021fu@somewhere.example.org>
Subject: Re: Are you available?

Sure, how can I help you?
```

The victim showed a reaction, so now she is hooked. The fake professor's second e-mail will arrive promptly.

```
From: John Doe <director2021fu@somewhere.example.org>
To: p_parker@fu...
Subject: Re: Are you available?

Okay, I need you to complete a task for me discreetly. I am in a meeting
now. Calls are prohibited, hence, I can only contact you via mail, I
have no idea when we will finish things here, however, I really need
your help with something that requires my urgent attention remotely.

[...]
```

Now the victim is in a fix. It doesn't really matter if she answers or not (in this example she does).

```
From: Petra Parker <p_parker@fu...>
To: John Doe <director2021fu@somewhere.example.org>
Subject: Re: Are you available?

OK. My next course starts at 2pm. I have some time now.

[...]
```

The attacker's third e-mail message is sure to come. It contains the actual scam.

```
From: John Doe <director2021fu@somewhere.example.org>
To: p_parker@fu...
Subject: Re: Are you available?

I need you to help me get gift cards from any store, I will reimburse
you when I get to the office. I need to send it to a colleague and it is
very important cause I'm still at the meeting and I need to get it sent
ASAP. Can you do that for me please ?

[...]
```

This is only an example mail-thread of course. It can be varied and go on for a couple of iterations longer. If the victim spends her private money on gift cards and sends the codes to the attacker at the end, she will be never see her money again.

Counter-Measures

Even though there is a high level of spam and virus scanning at Freie Universität Berlin that prevents many malicious e-mails from making it to your inbox, it is impossible to completely identify and block these kind of phishing mails.

Stay alert and do not fall for CEO fraud or other kinds of phishing attempts.

More informationen on ZEDAT Security- and Abuse-Management is available (in German) at:

https://www.zedat.fu-berlin.de/AbuseManagement

Informationen on personal certificates that make it possible to sign e-mails so they can be technically identified as valid by recipients is available (in German) at:

https://www.zedat.fu-berlin.de/Zertifikate